(19) RU (11) 2097931 (13) C1

(51) 6 H 04 L 9/00

Комитет Российской Федерации
по патентам и товарным знакам

ВСЕРОССИЙСКАЯ
ПАТЕНТНО-ТЕХНИЧЕСКАЯ
БИБЛИОТЕКА

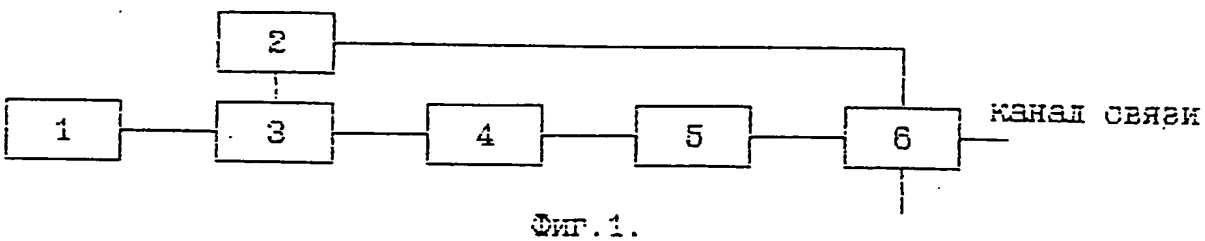
(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ
к патенту Российской Федерации

(21) 95100567/09 (22) 12.01.95
(46) 27.11.97 Бюл. № 33
(76) Березин Борис Владимирович, Волков Сергей Сергеевич, Рощин Борис Васильевич, Сердюков Петр Николаевич
(56) 1. Сяо Д., Керр Д., Мэдник С. Защита ЭВМ. - М.: Мир, 1982, с.137 - 162.

(54) СПОСОБ ШИФРОВАНИЯ ДВОИЧНОЙ ИНФОРМАЦИИ И УСТРОЙСТВО ДЛЯ ЕГО ОСУЩЕСТВЛЕНИЯ

(57) Изобретение относится к криптографическим преобразованиям и может быть использовано в связных, вычислительных и информационных системах для криптографического закрытия двоичной информации. Технический результат - обеспечение побитного шифрования информации с использованием ключа необходимого пользователю размера. Сущность изобретения заключается в многократном прибавлении ключа к преобразуемой информации с последующим применением подстановочных и перестановочных преобразований. Устройство содержит на передаче и приеме n-разрядный ключевой регистр 1, n-разрядный регистр сдвига 2, n-разрядный сумматор 3, блок 4 разрядного функционального преобразования f, мажоритарный элемент 5, однородный сумматор. 2 с. и 2 з.п. ф-лы, 2 ил.

RU 2097931 C1



Фиг. 1.

RU 2097931 C1

Изобретение относится к криптографическим преобразованиям и может быть использовано в связных, вычислительных и информационных системах для криптографического закрытия двоичной информации.

Известен способ шифрования, предназначенный для криптографической защиты информации в системах связи и вычислительных системах и заключающийся в многократном прибавлении ключа к преобразуемой информации с последующим применением подстановочных и перестановочных преобразований. С использованием этого способа построена система Lucifer фирмы IBM и стандарт шифрования данных Национального бюро стандартов США.

В известном стандарте шифрования данных к содержимому двух 32-разрядных ячеек 64-разрядного информационного регистра 16 раз прибавляют по модулю 2 содержимое 64-разрядного ключевого регистра с последующим воздействием на 32-разрядную сумму 32-разрядным функциональным преобразованием f.

Известный стандарт шифрования данных шифрует информацию блоками по 64 бита, а это при зашифровании требует предварительного накапливания 64 бит информации, а при расшифровании требует дополнительной синхронизации для выделения начала очередного блока зашифрованной информации. Кроме того, процесс зашифрования очередного блока состоит из 16-и циклов, что вносит определенную задержку при зашифровании очередных блоков информации. Перечисленные особенности известного стандарта шифрования данных делают его неудобным при использовании в системах радиосвязи.

Целью настоящего изобретения является обеспечение побитного шифрования информации с использованием ключа необходимого пользователю размера.

Поставленная цель достигается тем, что в способе шифрования двоичной информации, заключающемся в зависящем от 64-разрядного ключа преобразовании 64-разрядного блока шифруемой информации путем 16-кратного выполнения набора операций, включающего сложение 32-разрядных чисел из информационного и ключевого регистра и функциональное преобразование полученной 32-разрядной суммы, на передаче n-разрядные содержимые n-разрядного ключевого регистра и n-разрядного регистра сдвига складывают (например по модулю 2 либо 2^n), сумму преобразуют блоком n-разрядного функционального преобразования f, в полученном n-разрядном результате преобразования мажоритарным элементом определяют преобладание нулей или единиц и в зависимости от результата прибавляют по модулю 2 к двоичному знаку шифруемой информации соответственно 0 или 1, полученный в результате зашифрованный двоичный знак направляют в канал связи и на вход n-разрядного регистра сдвига, а на приеме выполняют те же действия, что и на передаче, за исключением того, что на вход n-разрядного регистра сдвига направляют пришедший из канала связи зашифрованный двоичный знак, к которому одновременно прибавляют по модулю 2 выработанный мажоритарным элементом двоичный знак и получают знак открытой информации. Чтобы мажоритарный элемент однозначно реагировал на поступающее на его вход число, разрядность числа n выбирается нечетной.

На фиг. 1 и 2 представлены соответственно блок-схемы устройств зашифрования и расшифрования для осуществления способа шифрования двоичной информации.

Устройства зашифования и расшифрования сдержат n-разрядный ключевой регистр 1, n-разрядный регистр сдвига 2, n-разрядный сумматор 3, блок n-разрядного функционального преобразования 4, мажоритарный элемент 5 и одноразрядный сумматор 6.

Процесс зашифрования бита открытой информации осуществляют следующим образом.

n-Разрядные содержимые n-разрядного ключевого регистра 1 и n-разрядного регистра сдвига 2 складывают (например по модулю 2 либо 2^n) в n-разрядном сумматоре 3, полученную сумму преобразуют блоком 4 n-разрядного функционального преобразования f, мажоритарным элементом 5 определяют количество единиц в n-разрядном результате преобразования. Если единиц больше, чем нулей, то в одноразрядном сумматоре 6 к двоичному знаку открытой информации прибавляют 1, в противном случае - 0. Полученный в результате суммирования двоичный знак зашифрованной информации направляют в канал связи и на вход n-разрядного регистра сдвига 2, содержимое которого предварительно сдвигают на один разряд в сторону младших разрядов с потерей выдвинутого самого младшего разряда.

Процесс расшифрования бита зашифрованной информации осуществляют следующим образом.

Best Available Copy

n-Разрядные содержимые n-разрядного ключевого регистра 1 и n-разрядного регистра сдвига 2 складывают в n-разрядном сумматоре 3, полученную сумму преобразуют блоком 4 n-разрядного функционального преобразования f, мажоритарным элементом 5 определяют количество единиц в n-разрядном результате преобразования. Если единиц больше, чем нулей, то в одноразрядном сумматоре 6 к пришедшему из канала связи знаку зашифрованной информации прибавляют 1, в противном случае - 0. В результате суммирования получают двоичный знак открытой информации. Пришедший из канала связи знак зашифрованной информации одновременно направляют на вход n-разрядного регистра сдвига 2, содержимое которого предварительно сдвигают на один разряд в сторону младших разрядов с потерей выдвинутого самого младшего разряда.

Если в i-й момент n-разрядный ключевой регистр 1 содержит n-разрядное число $k(i) = (k_1(i),...,k_n(i))$, $k_j(i) = 0,1$, $1 \le j \le n$, $i \ge 1$, то в i-й момент мажоритарный элемент вырабатывает двоичный знак $\gamma(i) = M(f(a(i)+k(i))$, где $M(a)=\{0$, если $|a|<n/2$; 1, если $|a|>n/2\}$, $|a|$ - количество единиц в n-разрядном двоичном числе a.

Если $o(i)$ = i-й двоичный знак открытой информации, $ш(i)$ - i-й двоичный знак зашифрованной информации, то $ш(i) = o(i) \oplus \gamma(i)$ на передаче и $o(i) = ш(i) \oplus \gamma(i)$ на приеме.

Содержимое n-разрядного регистра сдвига 2 в (i+1)-й момент станет $c(i+1) = (c_1(i+1) = c_2(i),...,c_{n-1}(i+1) = c_n(i+1) = ш(i))$.

Содержимое n-разрядного ключевого регистра 1 от такта к такту можно обновлять, например, при помощи регистра сдвига с линейной функцией в обратной связи. Если характеристический многочлен регистра имеет вид $1 \oplus x^{l-1}_{1} \oplus ... \oplus x^{l-1}_{s} \oplus x^{l-1}_{n}$, то в (i + 1)-й момент содержимое n-разрядного ключевого регистра 1 станет

$$k(i+1) = (k_1(i+1) = k_2(i),...,k_{n-1}(i+1) = k_n(i),\ k_n = (i+1) = k_1(i) \oplus k_{l_1}(i) \oplus ... \oplus k_{l_s}(i)).$$

В качестве n-разрядного функционального преобразования f можно выбрать, например, прибавление по модулю 2^n к преобразуемому n-разрядному числу $x = (x_1,...,x_n)$ n-разрядной константы a или n-разрядной константы b в зависимости от четности количества единиц в преобразуемом n-разрядном числе. Тогда $f(x) = x+x'a+(x' \oplus 1)b$,

где

$$x' = \oplus \sum_{j=1}^{n} x_j,\quad a = 2^{n-2} + 2^{n-4} + ... + 2^3 + 2^1,\quad b = 2^{n-1} + 2^{n-3} + 2^2 + ... + 2^1 + 1.$$

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ шифрования двоичной информации, заключающийся в зависящем от 64-разрядного ключа преобразования на передаче и приеме 64-разрядного блока шифруемой информации путем 16-кратного выполнения набора операций, включающего сложение 32-разрядных чисел из информационного и ключевого регистров и функциональное преобразование полученной 32-разрядной суммы, ***отличающийся*** тем, что на передаче n-разрядные содержимые n-разрядного ключевого регистра и n-разрядного регистра сдвига суммируют, полученную сумму преобразуют блоком n-разрядного функционального преобразования f, в полученном n-разрядном результате преобразования мажоритарным элементом определяют преобладание нулей и единиц и в зависимости от результата прибавляют по модулю 2 к двоичному знаку шифруемой информации соответственно 0 или 1, полученный в результате зашифрованный двоичный знак направляют в канал связи и на вход n-разрядного регистра сдвига, а на приеме n-разрядные содержимые n-разрядного ключевого регистра и n-разрядного регистра сдвига складывают, полученную сумму преобразуют блоком n-разрядного функционального преобразования f, в полученном n-разрядном результате преобразования мажоритарным элементом определяют преобладание нулей и единиц и в зависимости от результата прибавляют по модулю 2 соответственно 0 или 1 к пришедшему из канала связи зашифрованному двоичному знаку, который одновременно направляют на вход n-разрядного регистра сдвига.

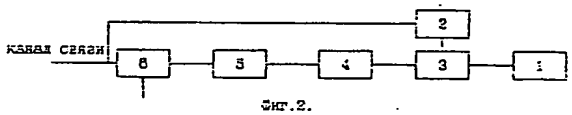
2. Способ по п.1, ***отличающийся*** тем, что блок функционального преобразования f в зависимости от четности количества нулевых разрядов в n-разрядном преобразуемом числе прибавляют по модулю 2^n к преобразуемому числу n-разрядную константу a или n-разрядную константу b.

3. Устройство шифрования двоичной информации, содержащее на приеме и передаче 8n-разрядный ключевой регистр, 8-разрядный блок функционального преобразования f и два 8-разрядных сумматора, ***отличающееся*** тем, что на приеме и

Best Available Copy

передаче введены n-разрядный регистр сдвига и мажоритарный элемент, вырабатывающий знак 0 при передаче на его вход n-разрядного числа с преобладанием нулевых разрядов и знак 1 при подаче на вход мажоритарного элемента n-разрядного числа с преобладанием единичных разрядов, при этом ключевой регистр выполнен в виде n-разрядного (n = 1, 3, 5 ...) ключевого регистра, блок функционального преобразования выполнен в виде блока n-разрядного функционального преобразования f, первый сумматор выполнен в виде n-разрядного сумматора, а второй сумматор - в виде одноразрядного сумматора, причем на передаче выход n-разрядного ключевого регистра подключен к первому входу n-разрядного сумматора, второй вход которого подключен к выходу n-разрядного регистра сдвига, вход которого подключен к выходу одноразрядного сумматора, вход которого подключен к выходу мажоритарного элемента, вход которого подключен к выходу блока n-разрядного функционального преобразования f, вход которого подключен к выходу n-разрядного сумматора, а на приеме выход n-разрядного ключевого регистра подключен к первому входу n-разрядного сумматора, второй вход которого подключен к выходу n-разрядного регистра сдвига, а выход n-разрядного сумматора подключен к входу блока n-разрядного функционального преобразования f, выход которого подключен к входу мажоритарного элемента, выход которого подключен к входу одноразрядного сумматора.

4. Устройство по п.3, *отличающееся* тем, что n-разрядный ключевой регистр выполнен в виде n-разрядного регистра сдвига с обратной связью с линейной функцией в обратной связи.



Фиг.2.

Best Available Copy

Заказ 371 Подписное
ВНИИПИ, Рег. ЛР № 040720
113834, ГСП, Москва, Раушская наб.,4/5

121873, Москва, Бережковская наб., 24 стр. 2.
Производственное предприятие «Патент»